Shadowserver threat update

Benedict Addis

LAC domain names week, 23rd September 2024

Case study 1: Machete

Summer 2019

SHADOWSERVER.ORG

ESET white paper July 2019

ESET Research White papers // July 2019

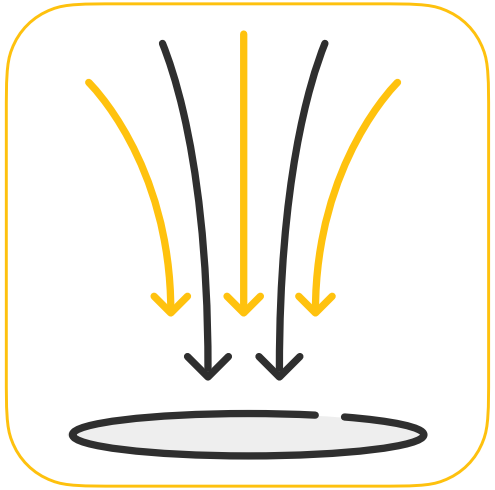
MACHETE JUST GOT SHARPER

Venezuelan government institutions under attack

How spies managed to steal gigabytes of confidential data over the course of a year

Machete disruption: a busy August 2019

- Received CEDIA (Ecuador) request
- Analyzed ESET report
- Identified 3 domains of interest
- Set up special sinkhole server
- Used ROLR contacts to redirect domains to sinkhole
- SUCCESS! First infected machines started to connect
- Validated incoming data
- Contacted CEDIA to report success, request contacts
- Shared data with EcuCERT, ColCERT and VenCERT
- Moved sinkhole to standard Shadowserver sinkholing infrastructure
- Added to standard Shadowserver reporting



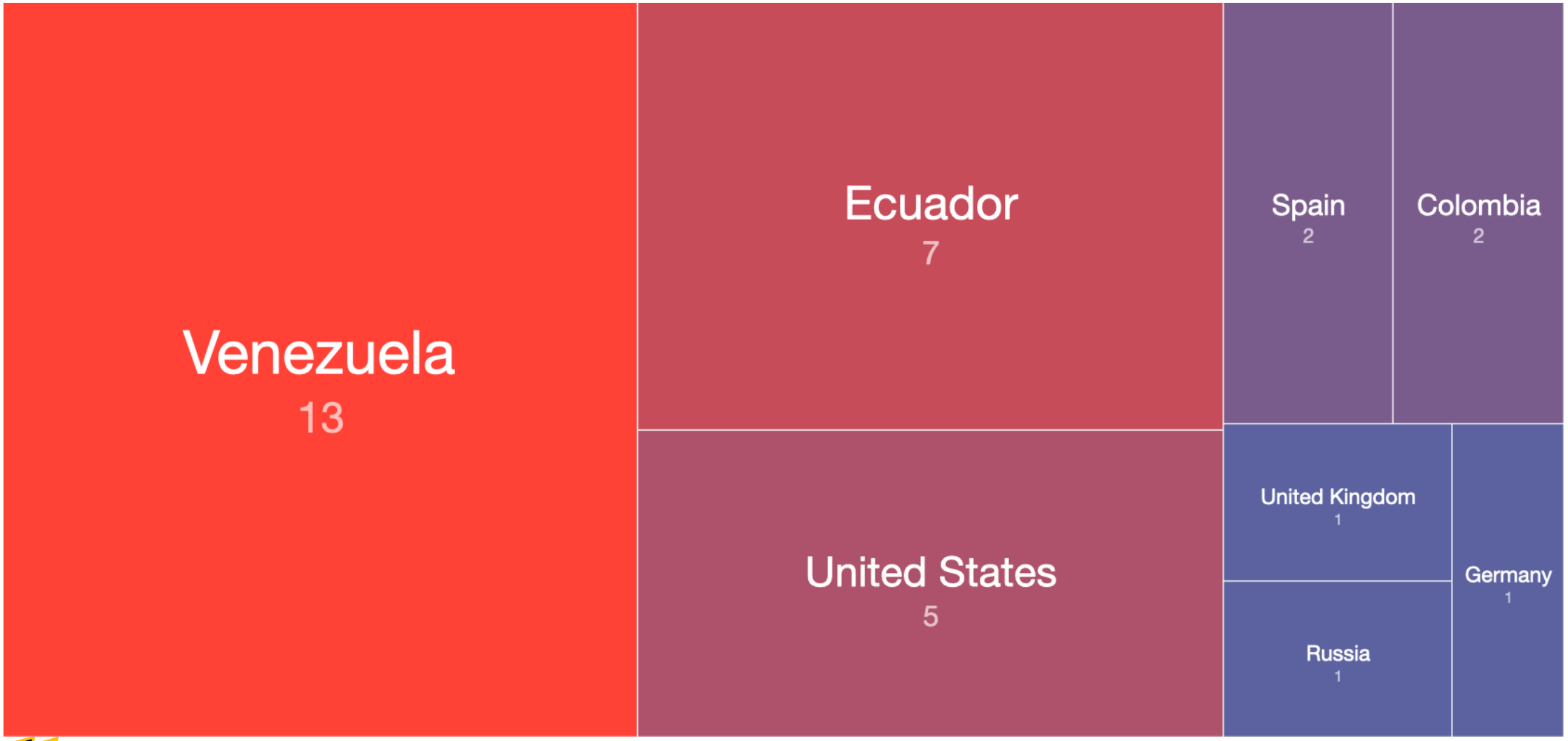
SHADOWSERVER

Machete infection map August 2019

SHADOWSERVER

TLP:Amber

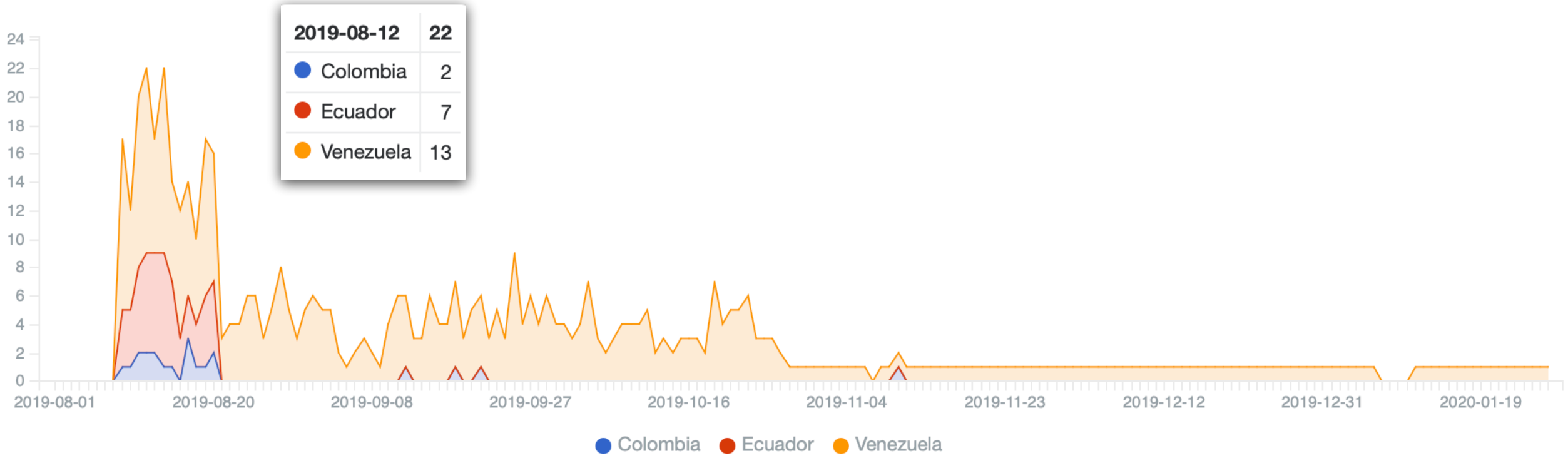
Machete victims



Numbers represent unique IPs seen on the day

TLP:Amber

Machete disruption



SHADOWSERVER

Case study 2: Android.Vo1d

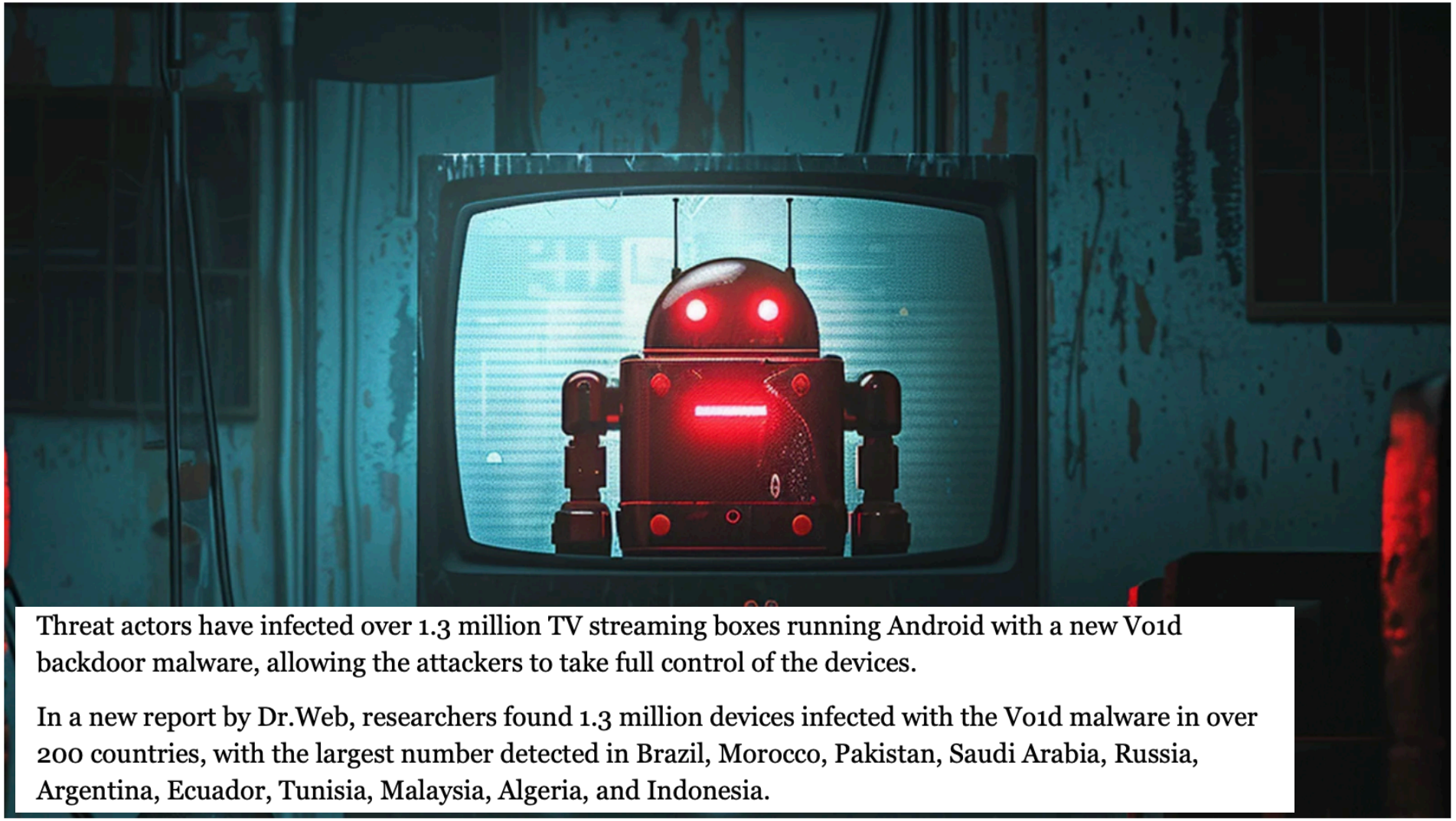
September 2024

SHADOWSERVER.ORG

New Vo1d malware infects 1.3 million Android streaming boxes

By **Lawrence Abrams**

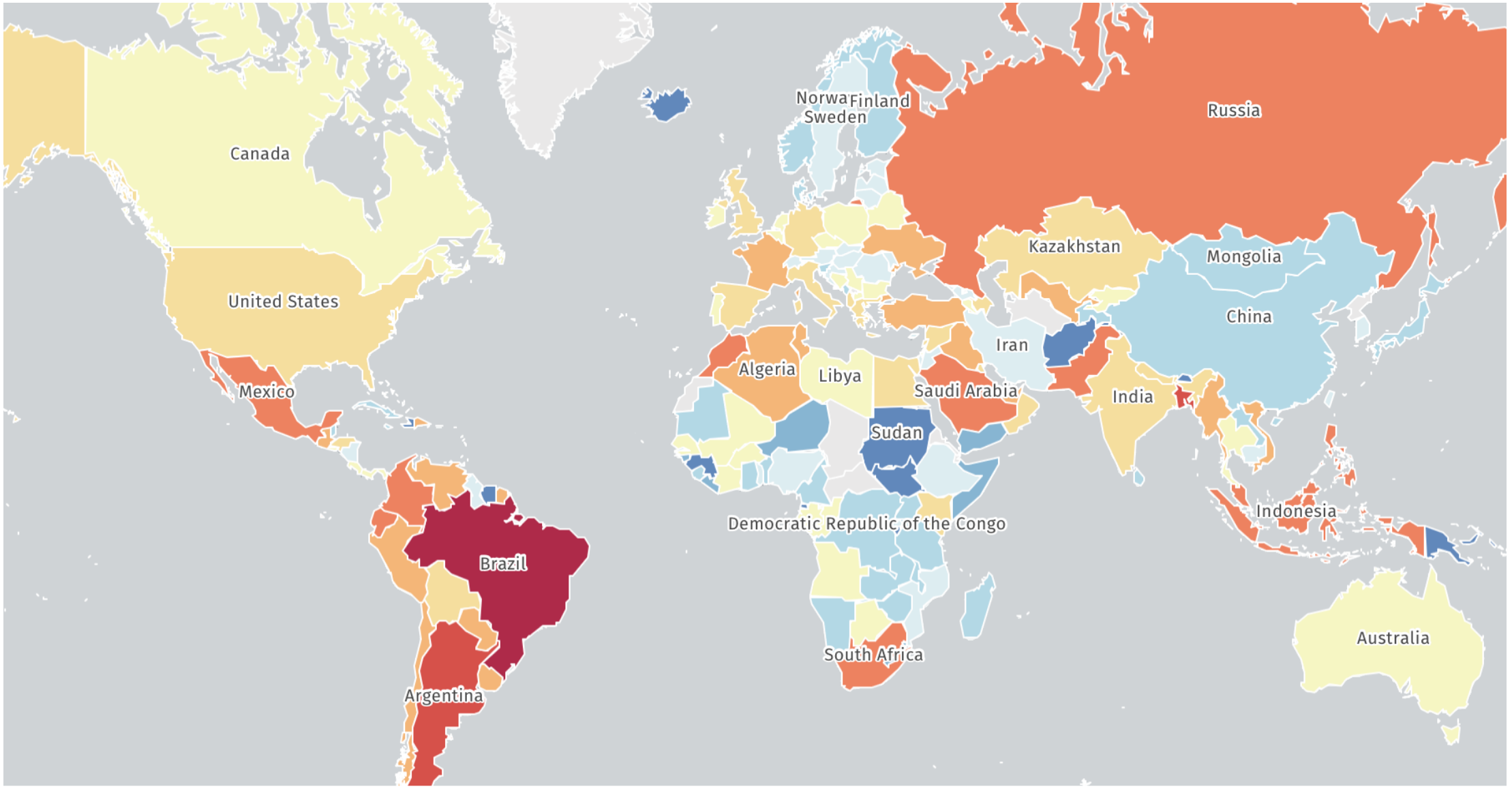
September 12, 2024 05:10 PM 1



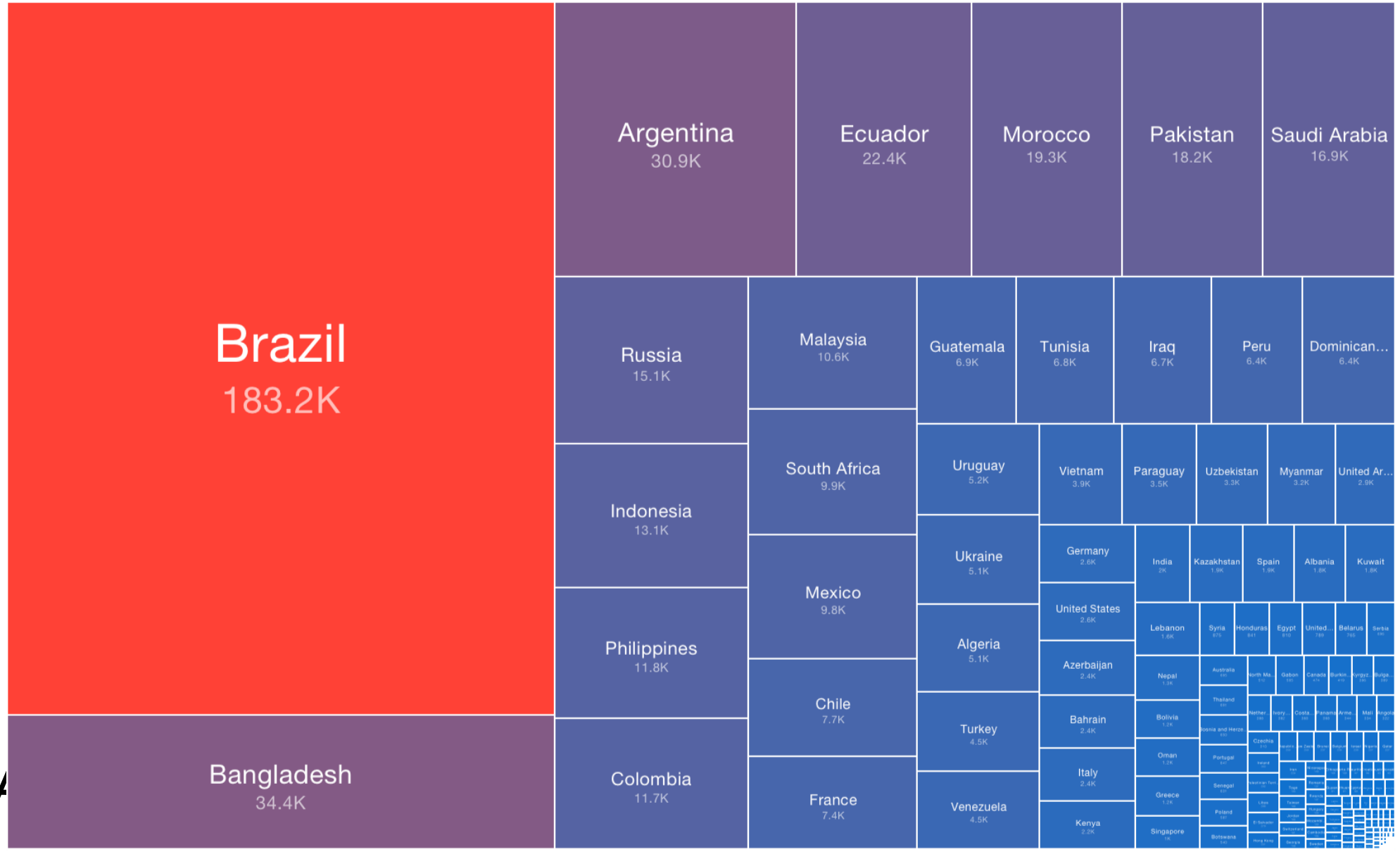
Threat actors have infected over 1.3 million TV streaming boxes running Android with a new Vo1d backdoor malware, allowing the attackers to take full control of the devices.

In a new report by Dr.Web, researchers found 1.3 million devices infected with the Vo1d malware in over 200 countries, with the largest number detected in Brazil, Morocco, Pakistan, Saudi Arabia, Russia, Argentina, Ecuador, Tunisia, Malaysia, Algeria, and Indonesia.

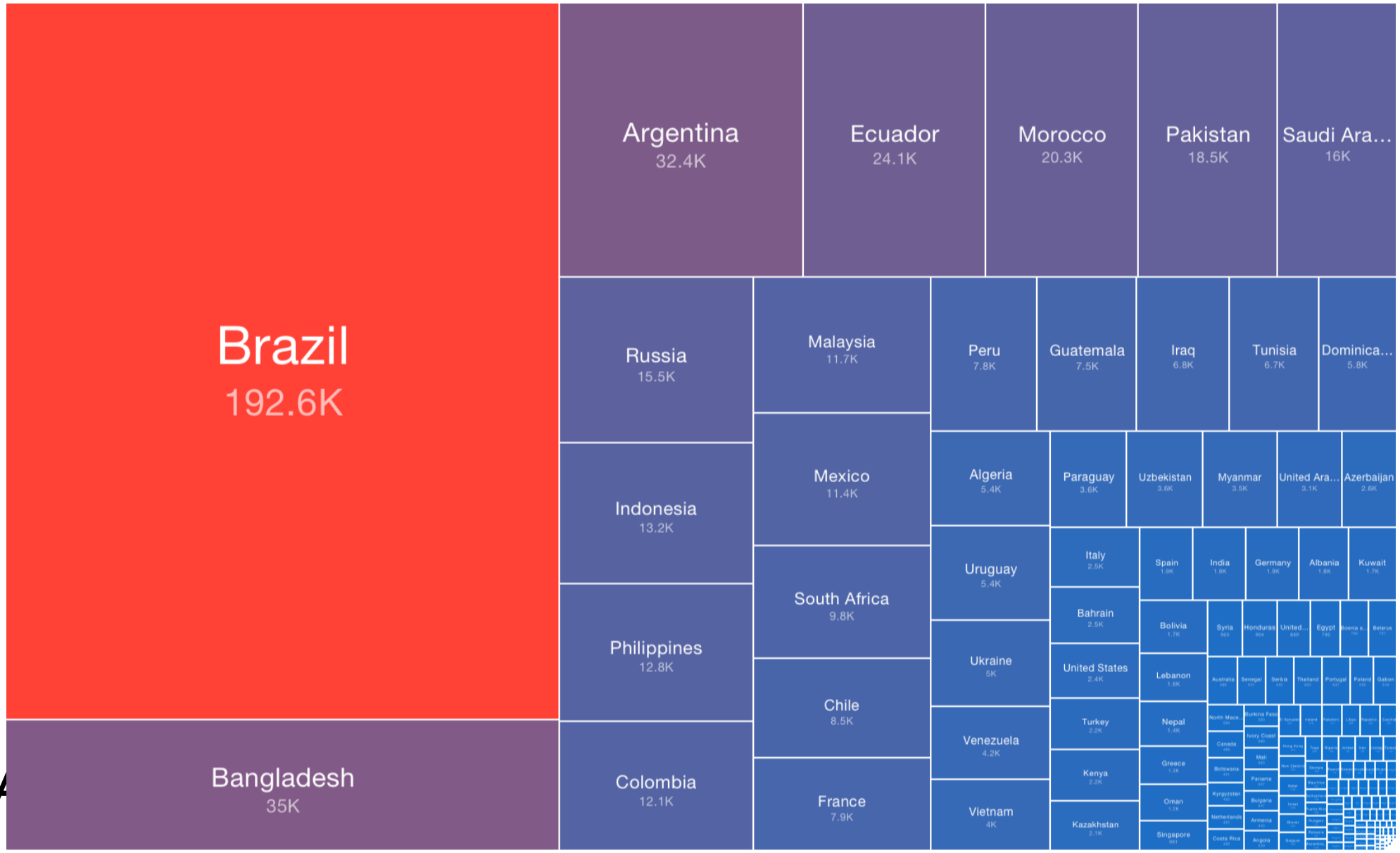
Vo1d victims map



Vo1d victims, 14th September 2024



Vo1d victims, 22nd September 2024



dashboard.shadowserver.org

Help us to sinkhole domains!

SHADOWSERVER

SHADOWSERVER

Lighting the way to a more secure Internet

@shadowserver

baddis@shadowserver.org

SHADOWSERVER.ORG